How-To Guide

Monitor Removable Media Devices in Logcollect

Publication Date
Nov 20, 2025

Abstract

This document provides instructions to enable the Removable Media Monitoring feature in Logcollect. It also explains the procedure for monitoring the activities of various removable media.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The Configuration details in this guide are consistent with Logcollect 9.x.

Audience

This guide is for the administrators responsible for monitoring and managing events in Logcollect.

Table of Contents

1 Overview

The USB and removable media are a vital part of any enterprise for data transfer. They have many forms such as flash memory drives, cell phones, cameras, and PDAs that can serve as storage devices. These portable devices are convenient for the transfer and storage of large data with or without network access. However, with these advantages, it has some security vulnerabilities. In the modern-day enterprise, USB data transfer is the simplest way of data theft. The chances of data leakage, creation of duplicate documents illegal data transfer, etc have also increased.

As an SIEM solution, Logcollect not only can monitor the USB or removable media device communications, but it also can identify the trusted USB and other devices. You can define the unique identifier number of the USB, so that the device will not be disabled upon insertion, and can access the information from the system.

2 Logcollect Monitoring Features

2.1 Reports Insertion/Removal of the Removable Devices

Logcollect will log every activity of the USB or other removable media devices like plug-in, plug-out, data transfer, etc. A complete audit trail that consists of the user, device type, serial number, time, and all the file activities is captured and sent as an event to the Logcollect Web console for processing.

2.2 Prevents Unauthorized Access and Reports the Intrusion in Real-time

Every time a USB is inserted, the Logcollect agent looks at the USB exception list, and if there is no violation of policy, it permits access to the device, while logging the insert activity. If a violation of policy is detected, access will be restricted, and the violation will be immediately sent to the Logcollect Web console. At this point, if access is permitted, Logcollect also begins to monitor all the activities of the device, and every file written to or deleted from the device will be recorded.

2.3 Restricts Access

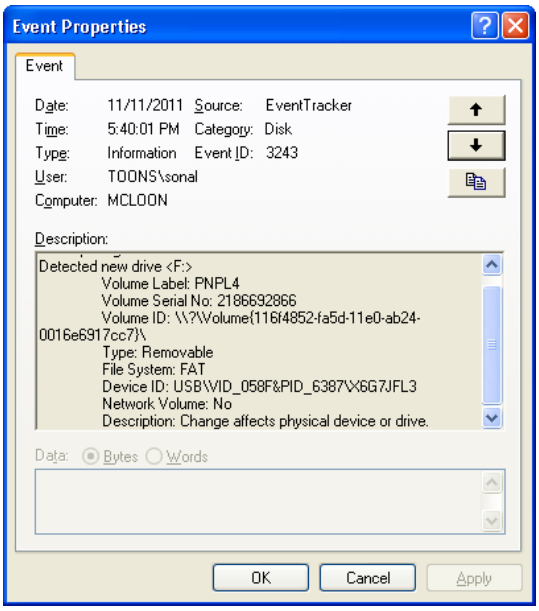
Logcollect can restrict access to all the USB devices on a system and can exempt the specified USB devices from monitoring which are added to the USB Exception list.

2.4 Protects the System from Malware

Logcollect can disable the USB or other removable media device upon insertion and thus safeguards the network from viruses and Trojans.

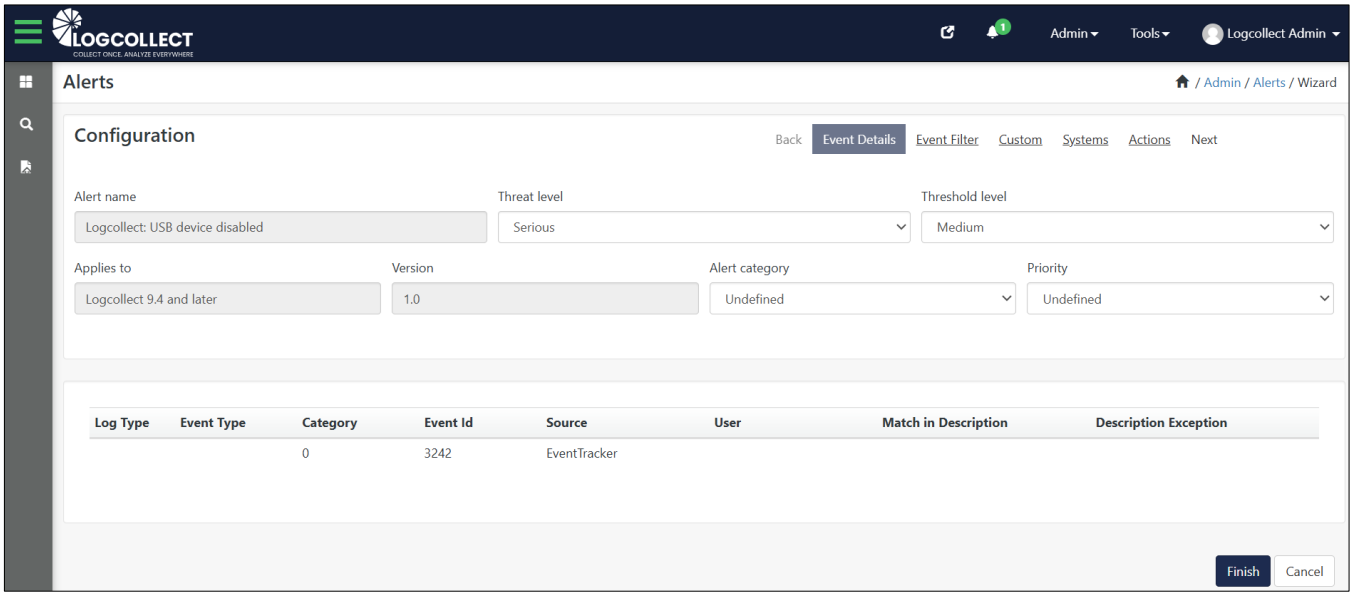
2.5 Logging USB Device Communication

For security and compliance purposes, Logcollect logs the USB communication in detail as incidents.



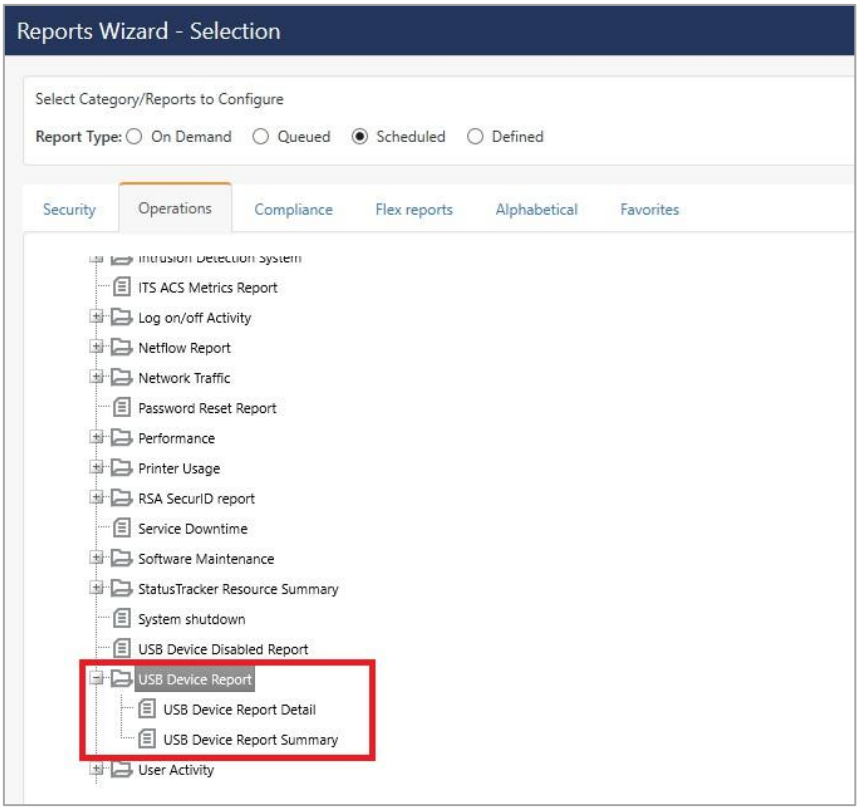
2.6 Alert Notification

In Logcollect, users can configure alerts to receive notifications upon the activities related to removable media.
Example: Logcollect: USB device disabled, Media Insert alert, etc.



2.7 Configures Media Insertion Report

Logcollect has a provision to configure the reports to analyze the removable media device activities. These reports help identify unauthorized access to the systems. To configure the USB device report, open **Logcollect > Operations > Reports**. In the **Report Tree**, click the **USB Device Report** node.



3 Enabling Removable Media Monitoring Feature

1. When a USB device is plugged in or media is inserted into the CD/DVD drive, Windows sends a media insertion notification with the drive name to the Logcollect Windows Agent.
2. Upon receiving the notification, Logcollect Windows Agent launches **USBTracker.exe** with drive details. **USBTracker.exe** is a Logcollect utility that monitors removable media file change activities.
3. **USBTracker.exe** generates **Event 3239** and starts monitoring all the activities (files added/modified /deleted/copied) that happen on the removable media.
4. When the USB device is unplugged or media is ejected, Windows sends a media removal notification to the USBTracker.exe.
5. Upon receiving the notification, USBTracker.exe stops monitoring and generates **Event 3240** with details of all activities.

Note

This feature is supported by Windows only and requires Logcollect Agent to be installed and configured.

3.1 Monitoring CDW/DVD Burning Activities

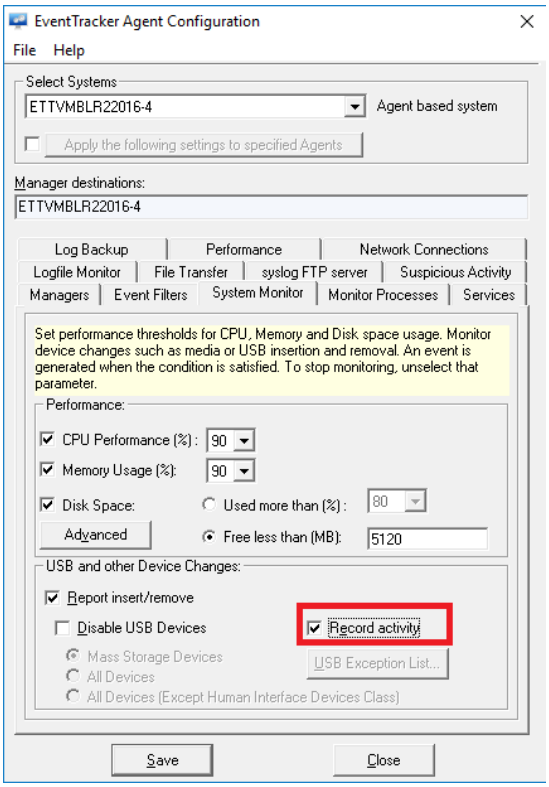
Windows has a built-in CD recorder feature that lets to drag and drop files using Windows Explorer to write files to a CD. Before burning the CD, Windows buffers the files in the 'staging area'. The staging area is a hidden folder that is usually "Drive letter:\Documents and Settings\Username\Local Settings\Application Data\Microsoft\CD Burning ".

3.2 Monitoring CD-ROM Activities

Windows captures the files copied from CD-ROM (CTRL + C or mouse right-click) to the clipboard. By monitoring the clipboard, you can keep track of the file copy activity.

3.3 Configuring Logcollect Agent to Monitor Removable Media

1. Click **Admin** and then select **Windows Agent Config**.
2. Select the desired system from the **Select System** dropdown list.
3. Click the **System Monitor** tab. The **Report insert/remove** checkbox is selected by default.
4. Select the **Record activity** checkbox under **USB and Other Device Changes**. This enables monitoring of all the removable media (USB, CD-R, CD-RW, and DVD) on the managed system.
5. Click **Save**. (Need to change the image)



Note

This option will report the device detected and device removal of Event IDs 3228 and 3229 for USB/Pen drives/External CDs, DVDs, etc. It will not report device detection and removal for mobile devices/External hard disk/Keyboard/Mouse.

3.3.1 Record Activity

Enabling this option will record the add/modify/delete activities from the hard disk to external devices. An Event ID 3240 will be generated. The supported devices are **Pen Drives, CDs, and DVDs.**

Note

It will not record any activity for External CDs, DVDs, and mobile devices.

3.3.2 Disable USB Devices

a. **Mass Storage Devices:** It will disable Pen Drives/External CDs or DVDs/Hard disks and Mobile devices (having Flash Drives and which do not have SD cards), connected as USB storage. For example, Non-Android Mobiles such as sm-b310e and Android mobiles of earlier versions such as the 2.0 series.

b. **All Devices:** It will disable Pen drives/External CDs or DVDs/Mouse/USB Headphones/ USB External CDs or DVDs except Keyboard.

c. **All Devices (Except Human Interface Devices Class):** All devices such as Pen drives/External CDs or DVDs/Mouse/USB Headphones/ USB External CDs or DVDs will be displayed **except Human Interface Devices (HIDs) which include Keyboard, Mouse, Joystick and Numeric Keypad.**

4 Exempt Authorized USB Drives

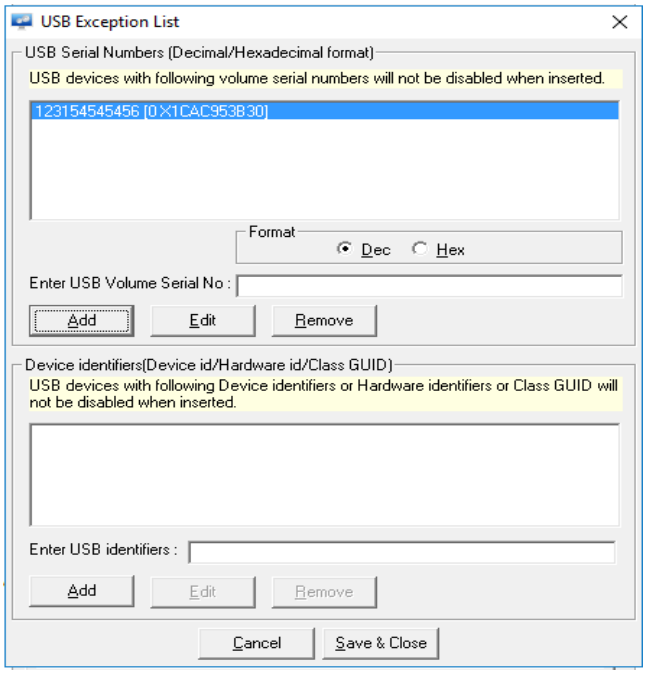
This option helps to restrict the users to use only authorized USB devices. Click the **USB Exception List**. Logcollect enables this button only when you select the disabled USB devices checkbox. Logcollect displays the USB Exception List pop-up window. The USB Exception list is divided into two sections:

4.1 USB Volume Serial Number

It will work for devices that possess volume levels such as the Pen Drive.

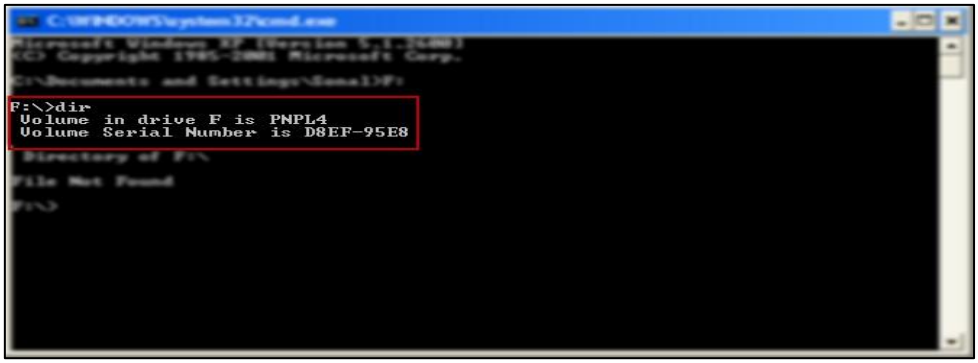
1. Select an appropriate **Format** option.
2. Type the serial number in the **Enter USB Serial number** field.
3. Click **Add**.

Logcollect adds the newly entered volume serial number to the exception list.

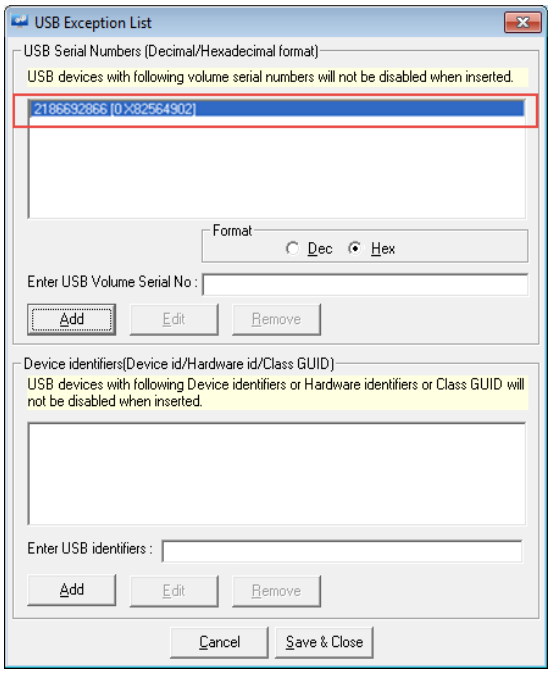


4.2 Finding USB Volume Serial Number

1. Verify if the USB device is inserted properly on the system.
2. Open **My Computer** and note the drive name for the USB device.
3. Open the command prompt and type the <drive name> of the USB drive.
4. Type "**dir**" to see the directory listing.



5. Note down the volume serial number shown in the **Hexadecimal** format.
6. In the **USB Exception list** window, enter this serial number in the **Enter USB Volume Serial number** text box.
7. Click the **Hex** option.
8. Click the **Add** button to add the serial number.



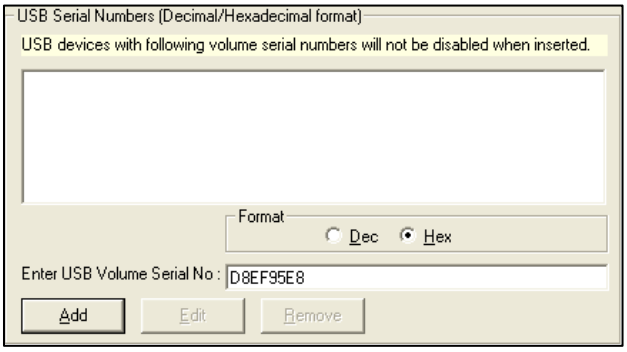
Note

- In the Command prompt, the volume serial number will always be in the 'Hexadecimal' format. You can convert it into Decimal format if required.
- It works only for Pen drives and no other mass storage devices.

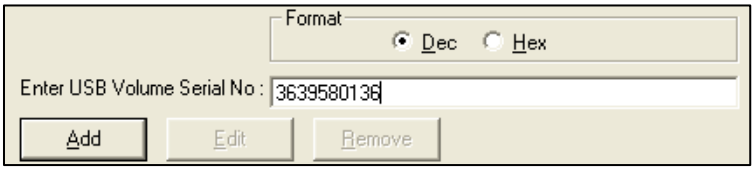
4.3 Converting USB Serial Number Format

You can convert the USB serial number from Hexadecimal to Decimal format, and vice versa.

1. Enter the USB serial number in the **USB Volume Serial No** field.



2. To convert the number into decimal format, click the **Dec** option. Logcollect automatically converts the number from Hexadecimal to Decimal format.



3. To convert the number again to hexadecimal format, click the **Hex** option.

Note

Logcollect will not allow you to enter an invalid number (containing an alphabet or symbols) when the decimal (**Dec**) option is selected.

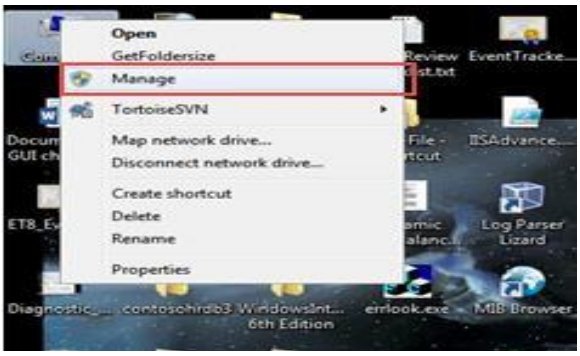
4.3.1 Device Identifiers (Device ID/ Hardware ID/ Class GUID)

The USB devices with the Device Identifiers - Device ID/Hardware ID/ Class GUID will not be disabled when inserted.

Device ID

It differs for all the devices. To add the Device ID to the exception list, perform the following steps:

1. Right-click **Computer** and select **Manage**.

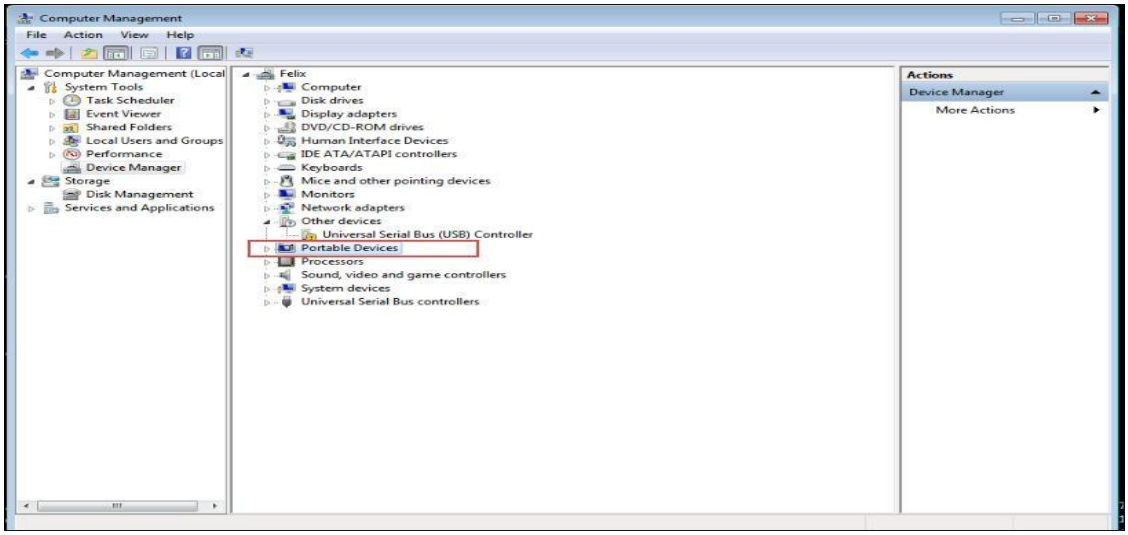


2. Select **Device Manager**.

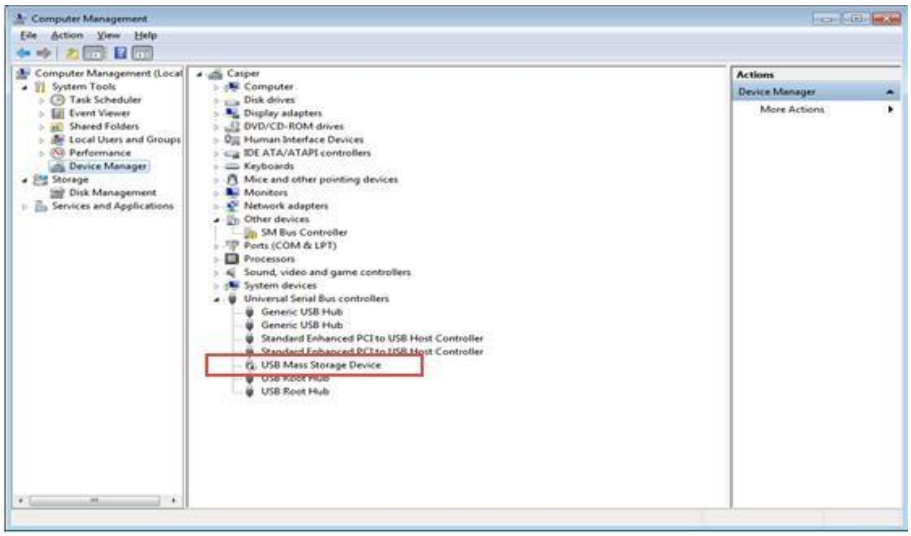
Note

Based on the device, select from the listed options.

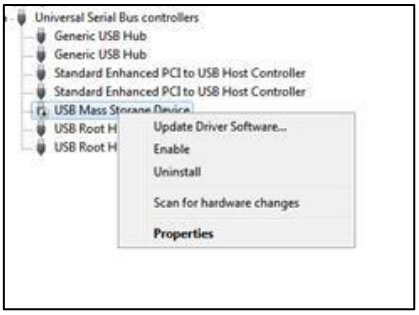
3. When the latest Android version mobile phones are connected, they will be displayed as “Portable Devices “. The screen is shown below:



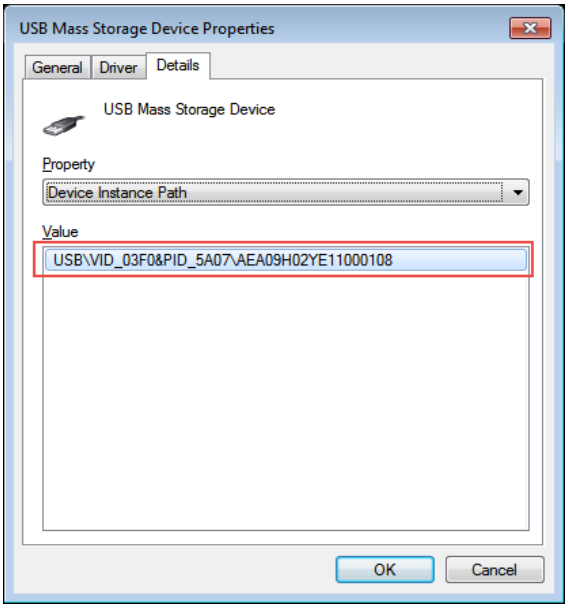
4. When the Android mobile phones of earlier versions such as 2.0 (with Flash devices) are connected, it will display within the **USB Mass Storage Device**. Here we have shown an example of a USB Mass storage Device.



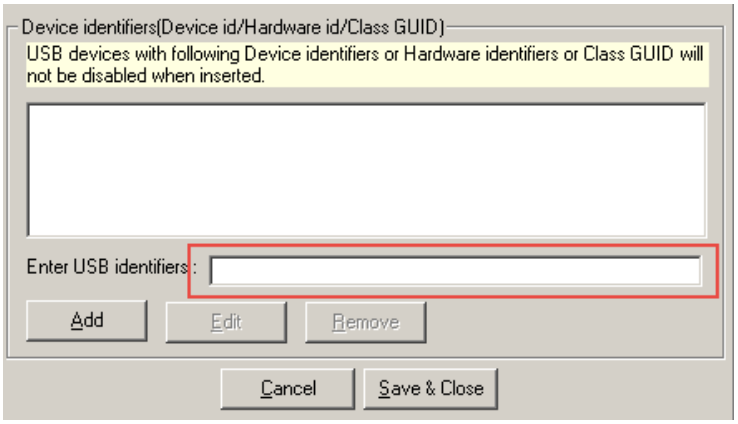
5. Right-click the **USB Mass Storage device**. Select **Properties**.



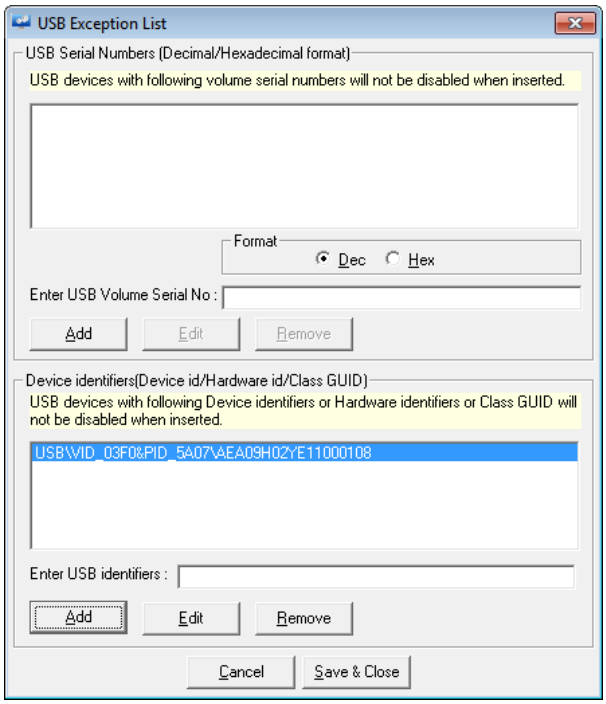
6. The USB Mass Storage Device Properties page will be displayed as shown below:
   a. Select the **Detail** tab.
   b. In the **Property** option, select **Device Instance Path** from the dropdown list.



c. Copy the **Value** highlighted in the figure above and paste it into the **Device Identifiers** field as displayed in the figure below:



7. Click the **Add** button.



Possible Substring Match for Device ID

The **disabled USB Devices** checkbox when clicked blocks the entry of all the USB devices. However, for authentic USB devices, we can add their USB serial number or Device ID to allow the USB data transfer. The following are the possible substring matches for the **Device ID** to allow more than one device at a time.

1. **To allow devices from a particular vendor:** Enter only the VID part like **USB\Vid_0781**
   In this example, 0781 is for SanDisk.
2. **To allow devices from a particular vendor and a particular product:**
   Enter VID and PID parts like **USB\Vid_0781&Pid_5567**

In this example, 5567 is for the SanDisk Cruzer Blade.

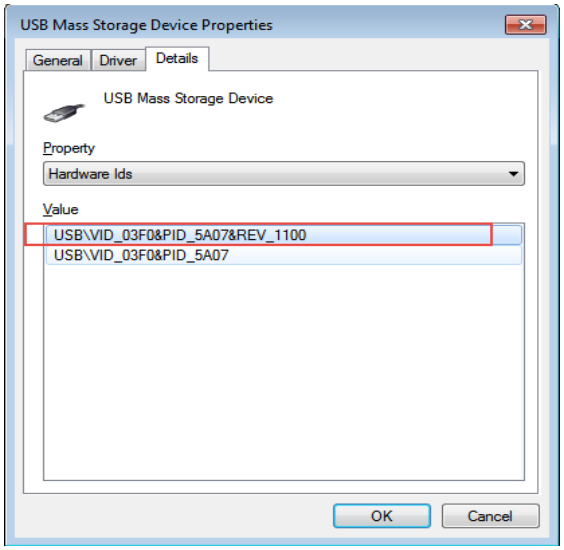
3. **To allow a device from a particular vendor and a particular product:**
   Enter VID, PID, and device serial number like **USB\Vid_0781&Pid_5567\20040203321B6B6256E9**.

   Click here for more details on PID/VID.

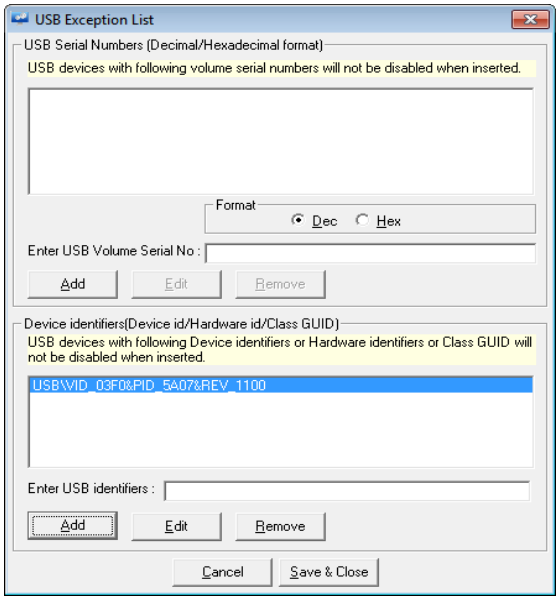
Hardware ID

Hardware ID remains the same for a device of the same class type but different for other class types. (e.g., the Hardware ID of the optical mouse will be the same, but the hardware ID of Lenovo, Dell, or HP will differ from each other). To add the Hardware ID to the exception list, perform the following steps:

1. Select the **Hardware ID** from the dropdown list in the **Property** section.



2. Copy the value and paste it in the **Device identifiers** field.
3. Click the **Add** button. It gets added and will be displayed as shown below:



Class GUID

Class GUID remains the same for a device class. (e.g. class GUID of the optical mouse will be the same for all whether it is Lenovo, Dell, or HP). The following is a table with the devices and their respective values.

Device	Value
Battery	{72631e54-78a4-11d0-bcf7-00aa00b7b32a}
Biometric device	{53D29EF7-377C-4D14-864B-EB3A85769359}
Bluetooth	{e0cbf06c-cd8b-4647-bb8a-263b43f0f974}
CDROM	{4d36e965-e325-11ce-bfc1-08002be10318}
Disk Drive	{4d36e967-e325-11ce-bfc1-08002be10318}
Display Device	{4d36e968-e325-11ce-bfc1-08002be10318}
FDC	{4d36e969-e325-11ce-bfc1-08002be10318}
Floppy Disk	{4d36e980-e325-11ce-bfc1-08002be10318}
HDC	{4d36e96a-e325-11ce-bfc1-08002be10318}
HIDClass	{745a17a0-74d3-11d0-b6fe-00a0c90f57da}
Dot4	{48721b56-6795-11d2-b1a8-0080c72e74a2}
Dot4Print	{49ce6ac8-6f86-11d2-b1e5-0080c72e74a2}
61883	{7ebefbc0-3200-11d2-b4c2-00a0C9697d07}
AVC	{c06ff265-ae09-48f0-812c-16753d7cba83}
SBP2	{d48179be-ec20-11d1-b6b8-00c04fa372a7}
1394	{6bdd1fc1-810f-11d0-bec7-08002be2092f}
Image	{6bdd1fc6-810f-11d0-bec7-08002be2092f}

Device	Value
Infrared	{6bdd1fc5-810f-11d0-bec7-08002be2092f}
Keyboard	{4d36e96b-e325-11ce-bfc1-08002be10318}
Medium Changer	{ce5939ae-ebde-11d0-b181-0000f8753ec4}
MTD	{4d36e970-e325-11ce-bfc1-08002be10318}
Modem	{4d36e96d-e325-11ce-bfc1-08002be10318}
Monitor	{4d36e96e-e325-11ce-bfc1-08002be10318}
Mouse	{4d36e96f-e325-11ce-bfc1-08002be10318}
Multifunction	{4d36e971-e325-11ce-bfc1-08002be10318}

Media	{4d36e96c-e325-11ce-bfc1-08002be10318}
MultiportSerial	{50906cb8-ba12-11d1-bf5d-0000f805f530}
Net	{4d36e972-e325-11ce-bfc1-08002be10318}
NetClient	{4d36e973-e325-11ce-bfc1-08002be10318}
NetService	{4d36e974-e325-11ce-bfc1-08002be10318}
NetTrans	{4d36e975-e325-11ce-bfc1-08002be10318}
SecurityAccelerator	{268c95a1-edfe-11d3-95c3-0010dc4050a5}
PCMCIA	{4d36e977-e325-11ce-bfc1-08002be10318}
Ports	{4d36e978-e325-11ce-bfc1-08002be10318}
Printer	{4d36e979-e325-11ce-bfc1-08002be10318}
Processor	{50127dc3-0f36-415e-a6cc-4cb3be910b65}
SCSIAdapter	{4d36e97b-e325-11ce-bfc1-08002be10318}
Sensor	{5175d334-c371-4806-b3ba-71fd53c9258d}
SmartCardReader	{50dd5230-ba8a-11d1-bf5d-0000f805f530}
Volume	{71a27cdd-812a-11d0-bec7-08002be2092f}
System	{4d36e97d-e325-11ce-bfc1-08002be10318}
TapeDrive	{6d807884-7d21-11cf-801c-08002be10318}
USB	{36fc9e60-c465-11cf-8056-444553540000}
Windows CE USB ActiveSync Devices (WCEUSBS)	{25dbce51-6c8f-4a72-8a6d-b54c2b4fc835}

Note

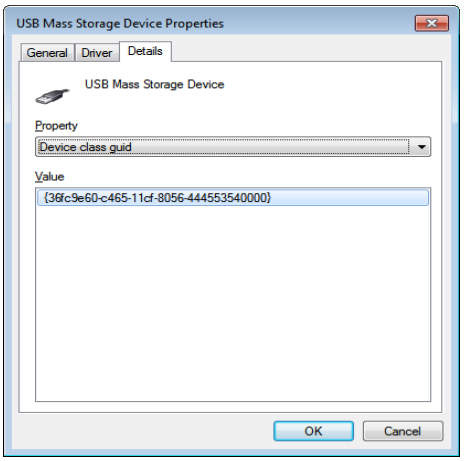
By providing the below device values, you can avoid disabling the mobile devices.

Devices	Value
Windows Portable Devices (WPD)	{eec5ad98-8080-425f-922a-dabf3de3f69a}
USB	{36fc9e60-c465-11cf-8056-444553540000}

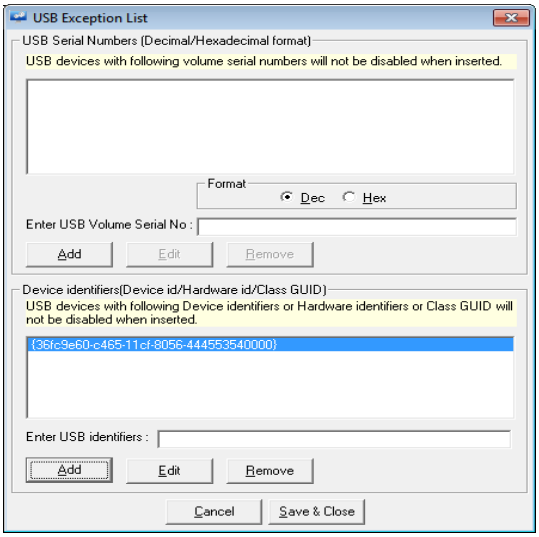
For References: https://msdn.microsoft.com/en-us/library/ff553426(VS.85).aspx

To add Class GUID to the exception list, perform the following steps.

1. Select **Device Class GUID** from the dropdown list.



2. Copy and paste the value in the **Device Identifier** field.
3. Click the **Add** button.



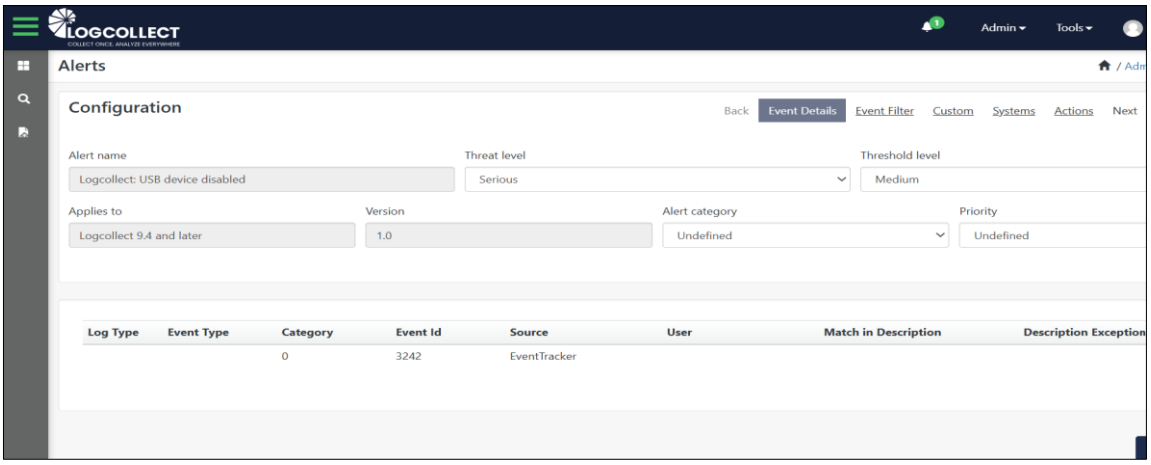
4. Click **Save & Close**.
5. Click **Save** on the System Monitoring page.

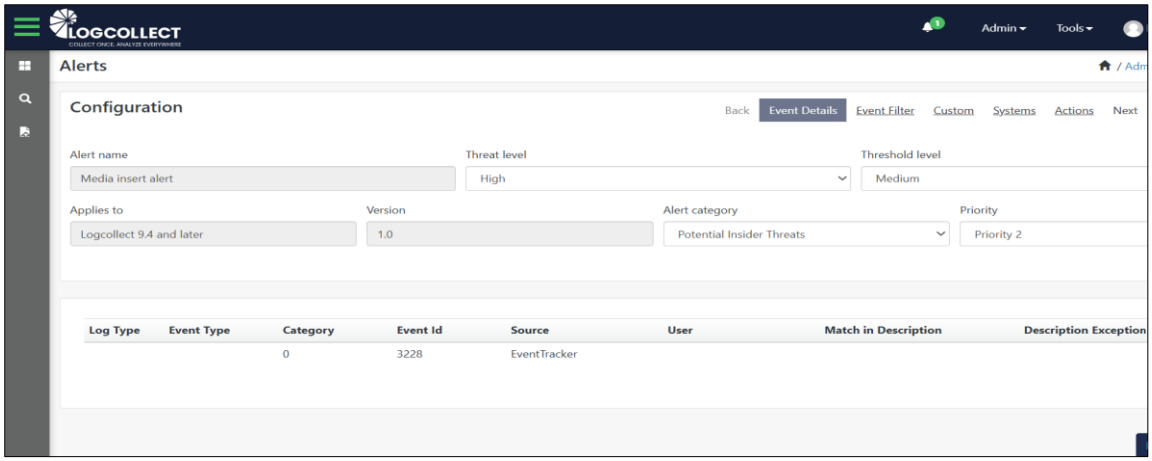
4.4 Configure Device Monitoring Alerts

The Device Monitoring Alerts can be configured to receive notifications. You can also view these Alert events on the Alerts Dashboard.

4.4.1 Configure USB Device Monitor Alerts

1. Click **Admin** and then select **Alerts**.
2. Locate **Logcollect: USB device disabled** & **Media Insert Alerts**.
3. Select the severity of the threat from the **Threat Level** dropdown list.
4. Select the checkbox under **Active**, if not selected.
5. Set appropriate alert actions to receive notifications.
6. Click **OK**.

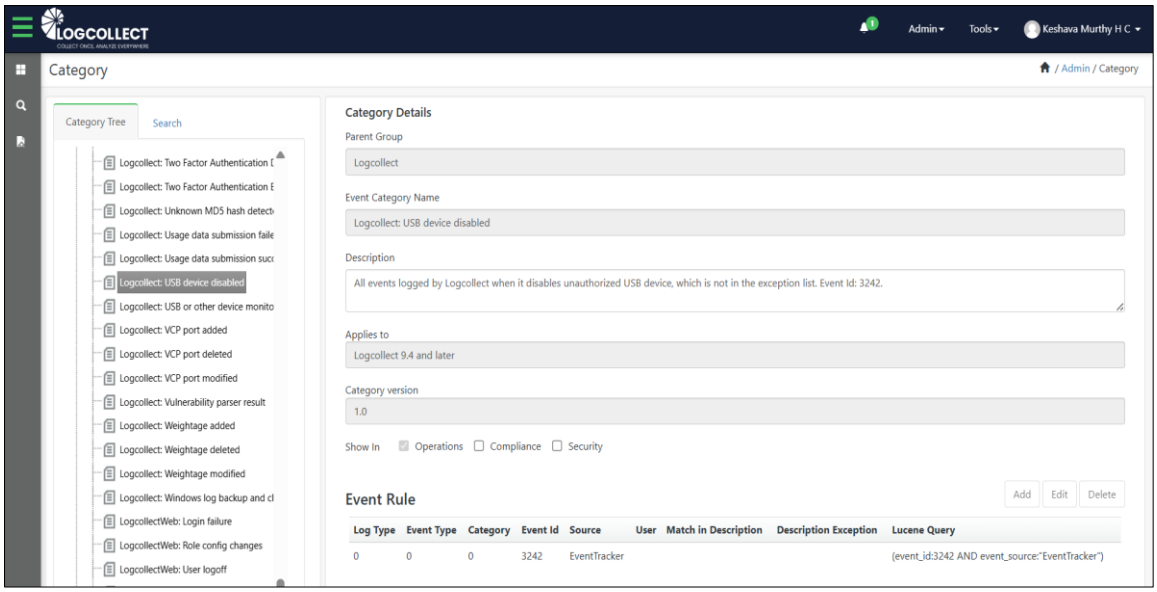




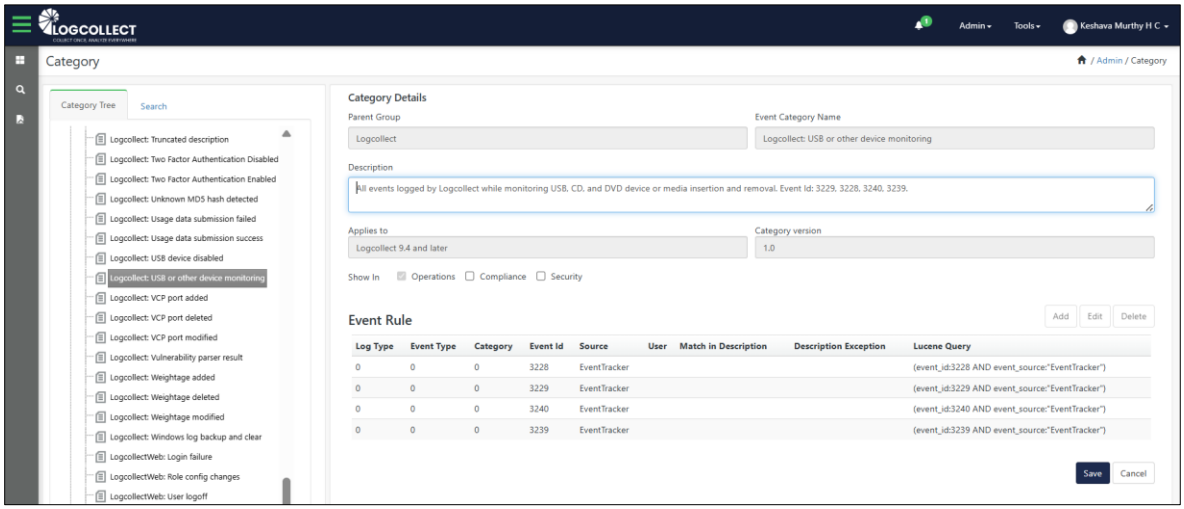
4.5 Logcollect Device Monitoring Categories

To view Categories, click **Admin** and then select **Category**.

Category: Logcollect: USB device disabled
Description: All the events logged by Logcollect when it disables the unauthorized USB devices, which is not in the exception list.
Event ID: 3242



Category: Logcollect: USB or other device monitoring
Description: All events logged by Logcollect while monitoring USB, CD, and DVD devices or media insertion and removal.
Event ID: 3228, 3229, 3239, 3240.



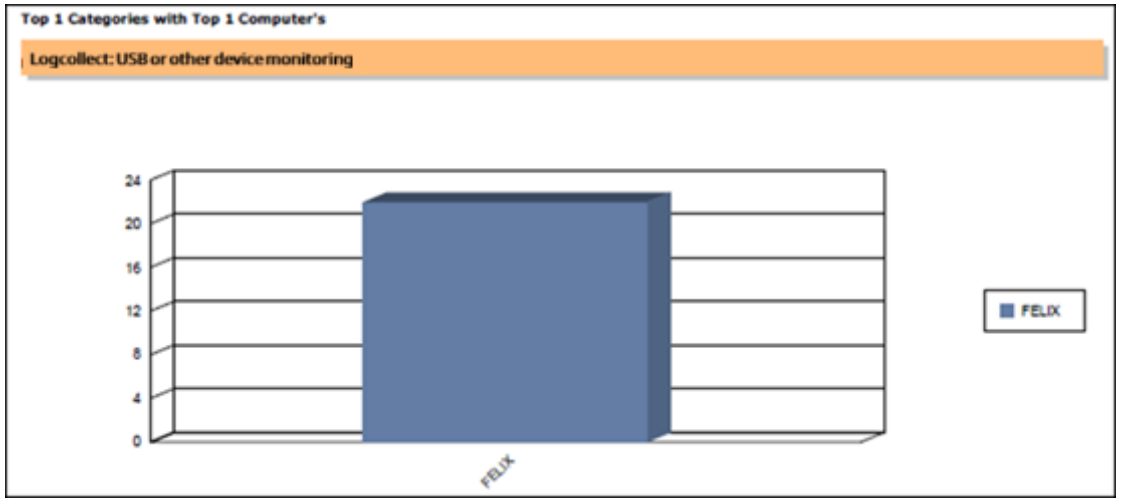
4.6 Logcollect Device Monitoring Reports

4.6.1 USB or Other Device Monitoring

Go to **Operations > Reports > Logcollect: USB or other device monitoring.**

Logcollect Agent for Windows can be configured to monitor insert/removal and files added/modified/deleted/copied to and from removable media. If this feature is enabled, this report provides information on those activities across selected computers for the selected period.

Usage: This report must be run and reviewed regularly for all critical servers and workstations.



Category Detail Report Sorted By Computer

Category Logcollect: USB or other device monitoring had 1 Computers generating 22 events

Event IDs included are 3228, 3229, 3239, 3240

Computer FELIX generated 22 events. Details of Events are given below.

Log Time	User	Event Id	Source	Event Description
9/7/2015 3:12:57 PM		3228	EventTracker	Detected new drive <F:> Device Type: Fixed Volume Label: FreeAgent GoFlex Drive Volume Serial No: 1546817573 Volume ID: \\?\Volume{8c5f0eaa-f5d0-11e4-bf06-fcf286e6e67f}\ File System: NTFS Device ID: USB\VID_0BC2&PID_5021\NA05SA8J Network Volume: No Description: Change affects physical device or drive. <EventData><Data>Detected new drive <F:> Device Type: Fixed Volume Label: FreeAgent GoFlex Drive Volume Serial No: 1546817573 Volume ID: \\?\Volume{8c5f0eaa-f5d0-11e4-bf06-fcf286e6e67f}\ File System: NTFS Device ID: USB\VID_0BC2&PID_5021\NA05SA8J Network Volume: No Description: Change affects physical device or drive.</Data></EventData>
9/7/2015 3:14:45 PM		3229	EventTracker	Drive <F:> removed. Network Volume: No Description: Change affects physical device or drive. <EventData><Data>Drive <F:> removed. Network Volume: No Description: Change affects physical device or drive.</Data></EventData>

4.6.2 USB Device Disabled Report

Go to **Operations > Reports > USB Device Disabled Report.**
This report provides information on the disabled USB devices across selected computers for the selected period.
Usage: This report would be useful when you are looking for a quick report on disabled USB devices.

Computer FELIX USB devices used is 5

Log Time	User	Device	Device ID
9/9/2015 6:42:22PM	[redacted]	USB Mass Storage Device	USB\VID_0951&PID_1629\0018F30C9F
9/9/2015 6:42:48PM	[redacted]	USB Mass Storage Device	USB\VID_0951&PID_1629\0018F30C9F
9/9/2015 6:43:25PM	[redacted]	USB Mass Storage Device	USB\VID_0951&PID_1629\0018F30C9F
9/9/2015 6:44:13PM	[redacted]	USB Mass Storage Device	USB\VID_0BC2&PID_5021\NA05SA8J
9/9/2015 6:44:42PM	[redacted]	USB Mass Storage Device	USB\VID_0BC2&PID_5021\NA05SA8J
9/9/2015 6:49:10PM	[redacted]	USB Input Device	USB\VID_17EF&PID_6019\6&25e9f07&(
9/9/2015 6:54:07PM	[redacted]	USB Input Device	USB\VID_0461&PID_4E22\6&25e9f07&(
9/9/2015 6:54:12PM	[redacted]	USB Input Device	USB\VID_0461&PID_4E22\6&25e9f07&(
9/9/2015 6:55:07PM	[redacted]	USB Input Device	USB\VID_0461&PID_4E22\6&25e9f07&(
9/9/2015 6:59:30PM	[redacted]	MTP USB Device	USB\VID_0FCE&PID_0180\YT9100L4LK

4.6.3 USB Device Report Details

Go to **Operations > Reports > USB Device Report > USB Device Report Detail.**
This report provides detailed information on the files added/modified/deleted to the USB device. It can be tuned by applying Refine or Filter criteria, systems, and time.
Usage: This report is usually run during a detailed investigation phase, as needed.

Computer FELIX Removable media devices used is 1

CD\DVD Device (E:\) with Serial No. 2663209342 active users is 1

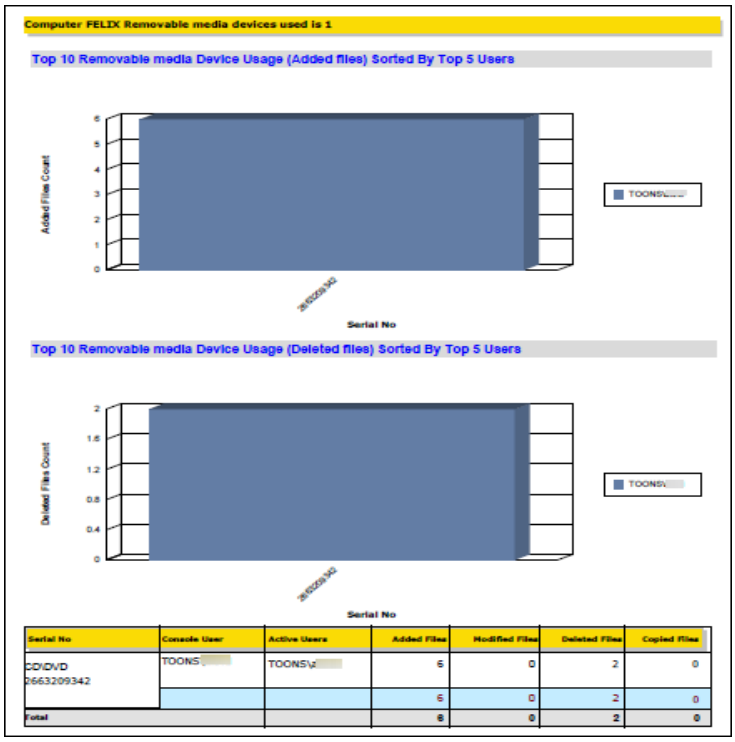
Console User TOONS\[redacted] file activities is 8

Active Users: TOONS\[redacted]

File Activity Time	File Activity	File/Folder Name
9/9/2015 06:47:50PM	Added	EventTracker USB or other device monitoring^329^1441622724.pdf
9/9/2015 06:47:50PM	Added	EventTracker USB or other device monitoring^329^1441622724.pdf
9/9/2015 07:09:54PM	Deleted	EventTracker USB or other device monitoring^329^1441622724.pdf
9/9/2015 07:09:54PM	Deleted	EventTracker USB or other device monitoring^329^1441622724.pdf
9/9/2015 07:10:29PM	Added	export usb device disabled.issch
9/9/2015 07:10:29PM	Added	export usb device disabled.issch
9/9/2015 07:10:42PM	Added	8.0 EventTracker1433054376_latest.cer
9/9/2015 07:10:42PM	Added	8.0 EventTracker1433054376_latest.cer

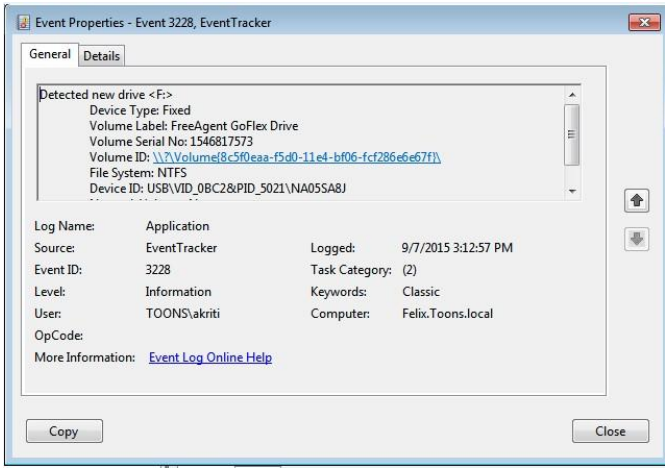
4.6.4 USB Device Report Summary

Go to **Operations > Reports > USB Device Report > USB Device Report Summary.**
This report provides a summary of the files added/modified/deleted to the USB device. The charts are included per system per activity, top 10 USB devices are sorted by the top 5 users.
Usage: This report would be useful when you are looking for a quick report for the files added/modified/deleted/copied to and from USB devices.



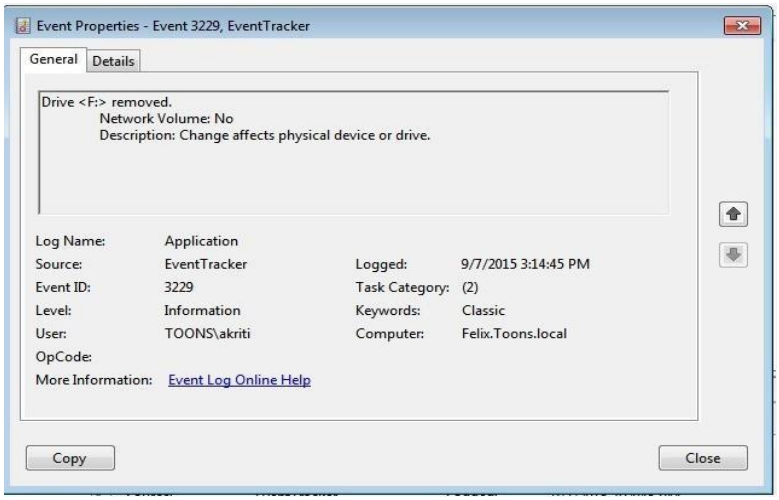
4.7 Logcollect Generated Events

Logcollect detects the new drive [3228] **(Need to change the image)**



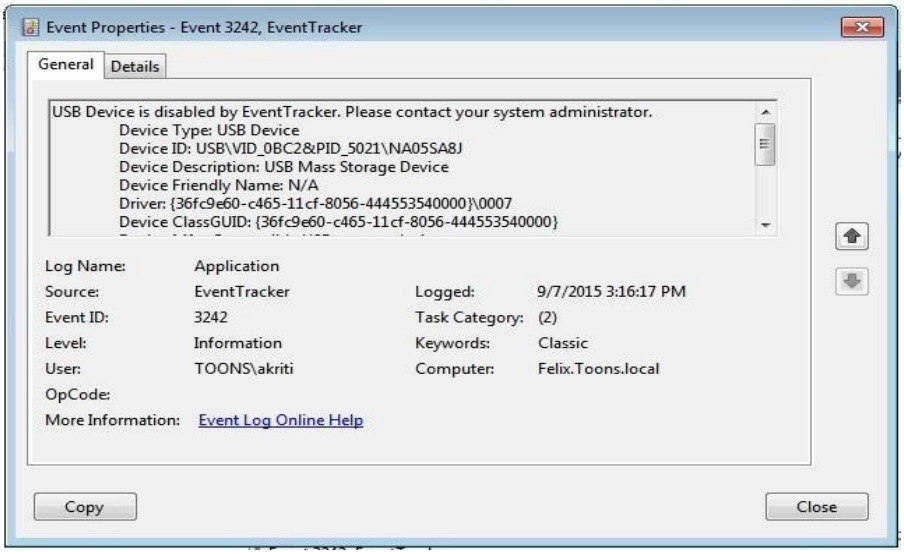
Details: Detected new drive <F:>
Device Type: Fixed
Volume Label: FreeAgent GoFlex Drive
Volume Serial No: 1546817573
Volume ID: \\?\Volume{8c5f0eaa-f5d0-11e4-bf06-fcf286e6e67f}\
File System: NTFS
Device ID: USB\VID_0BC2&PID_5021\NA05SA8J
Network Volume: No
Description: Change affects physical devices or drives.

Logcollect <drive name> removed [3229] **(Need to change the image)**



Details: Drive <F:> removed
Network Volume: No
Description: Change affects physical devices or drives.

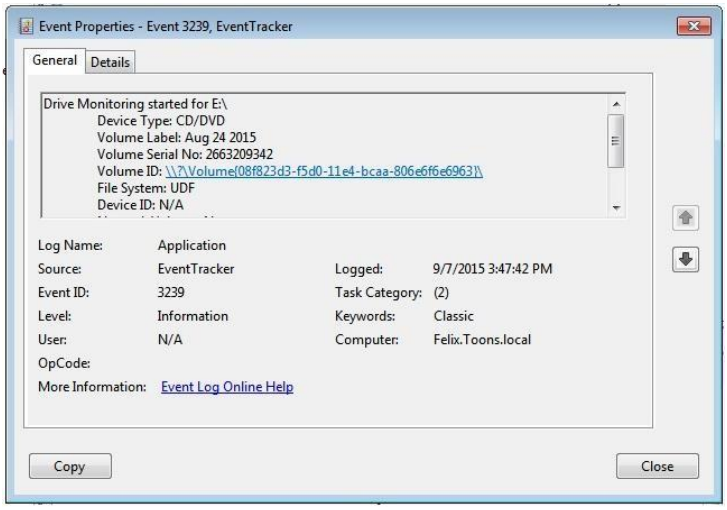
USB device is disabled by Logcollect [3242] **(Need to change the image)**



Details: USB Device is disabled by Logcollect. Please contact your system administrator. Device Type: USB Device
Device ID: USB\VID_0BC2&PID_5021\NA05SA8J
Device Description: USB Mass Storage Device
Device Friendly Name: N/A
Driver: {36fc9e60-c465-11cf-8056-444553540000}\0007
Device ClassGUID: {36fc9e60-c465-11cf-8056-444553540000}
Device Mfg: Compatible USB storage device
Hardware ID: USB\VID_0BC2&PID_5021&REV_0148
Enumerator: USB

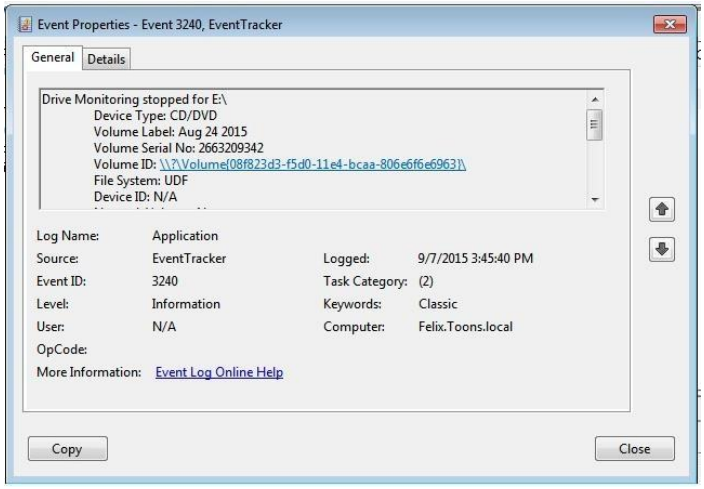
Local Information: Port_#0002.Hub_#0003
Physical Device Object Name: \Device\USBPDO-6
Service Name: USBSTOR
BUS Number: 0
Capability: Removable UniqueID RawDeviceOK SurpriseRemovalOK

USB Monitoring started for<drive name> [3239] **(Need to change the image)**



Details**:** Drive Monitoring started for E:\
Device Type: CD/DVD
Volume Label: Aug 24 2015
Volume Serial No: 2663209342
Volume ID: \\?\Volume{08f823d3-f5d0-11e4-bcaa-806e6f6e6963}\
File System: UDF
Device ID: N/A
Network Volume: No
Description: Change affects media in the drive.
Console User: TOONS\akriti
Active Users: TOONS\akriti

USB Monitoring stopped for<drive name> [3240] (Need to change the image)



Details: Drive Monitoring stopped for E:\
Device Type: CD/DVD
Volume Label: Aug 24 2015
Volume Serial No: 2663209342
Volume ID: \\?\Volume{08f823d3-f5d0-11e4-bcaa-806e6f6e6963}\
File System: UDF
Device ID: N/A
Network Volume: No
Description: Change affects media in the drive.
Console User: TOONS\akriti
Active Users: TOONS\akriti
Files copied by using Live File System: USBDeview|Added|09/07/2015 03:44:46 PM
Files accessed by user: TOONS\akriti desktop.ini|Existing|09/07/2015 02:23:19 PM

4.8 Limitations

Logcollect Windows Agent monitors CD/DVD burning activities carried only through Windows Explorer and does not monitor burning activities done via third-party tools such as Nero, Iomega, etc.

About Logcollect

Logcollect is a software-only telemetry pipeline which supports the collection, enrichment, transformation and routing of security data from sources to multiple destinations. It is targeted to security operations that are struggling with distributing large volumes of disparate data, high operational costs, alert fatigue and missed threats. It is available as a software license or hosted in AWS. It is backed by a team that has extensive experience with security logging, SIEM and regulatory compliance. Collect once, analyze everywhere.

Headquartered in Ft. Lauderdale, FL, Logcollect is a leader in Log Collection. Learn more at www.Logcollect.com.

Contact Us

Corporate Headquarters

Prism Microsystems
920 NE 17th Way
Fort Lauderdale, FL 33304

https://www.Logcollect.com/support